Bundesamt
für Sicherheit in der
Informationstechnik

Orientation Guide to Verification According to § 8a , Para. 3, BSI Act

Version 1.0
of 15 May 2019

Version history

Date	Version	Author	Remarks
07/10/2016	0.9	BSI	
20/10/2016	0.9.01	BSI	Minor corrections regarding layout and spelling
30/06/2017	0.9.02	BSI	Change to Chapter 5.4 Audit effort; Amendments to the Implementing Regulation on the NIS Directive
05/10/2017	0.9.03	BSI	References corrected
07/03/2019	0.9.7	BSI	• Incorporation of various comments • Sub-chapter "Legal basis" deleted as only a BSI Act quotation • A clearer description of the tasks and suitability of the auditing body and the audit team • Better explanation of the concepts of security deficiency, security category and implementation plan. Inclusion of a template of deficiencies. • (More detailed) description of the verification process, in particular on verification documents and deadlines
12/04/2019	0.9.9	BSI	• Consolidation in BSI • Incorporation of comments from TAK AS
15/05/2019	1.0	BSI	• Final agreement in BSI, creation of document accessibility

Federal Office for Information Security

P.O.B. 20 03 63
53133 Bonn
Phone: +49 22899 9582-0

E-mail: kritische.infrastrukturen@bsi.bund.de

Internet: https://www.bsi.bund.de

Table of contents

1 Overview

1.1 Introduction

Operators of critical infrastructures (KRITIS operators) must, in accordance with § 8a Para. 1 of the BSI Act (BSIG), provide the BSI with evidence in an appropriate manner of their precautions to avoid disruptions to the availability, integrity, authenticity and confidentiality of their information technology systems, components or processes which are crucial for the operability of the critical infrastructures they operate.

KRITIS operators must submit verification documents to the BSI for each registered system. These shall include both general information on the nature and extent of the audits carried out and a list of the security deficiencies detected.

According to § 8a Para. 3 BSIG "[...] the BSI may request the submission of the documentation on which the review was based. In the event of security deficiencies, in consultation with the competent federal regulatory authority or after consultation with the otherwise competent regulatory authority as necessary, the BSI may request that the security deficiencies be remedied." For issues that are not fully clarified, the BSI can also obtain its own impression of the KRITIS operator's security precautions through its own on-site audit in accordance with § 8a Para. 4 BSIG.

1.2 Objective of the orientation guide

The purpose of this document is to give guidance to operators of critical infrastructures and auditing bodies on what is meant by "*in an appropriate manner*" in § 8a Para. 3 BSIG in relation to an audit and how the legal requirements under § 8a Para. 3 BSIG can be met. It describes the requirements for the participants as well as their tasks and responsibilities and provides a framework for appropriate verification. It explains the procedure for the submission of supporting verification, the formal aspects to be observed and the deadlines to be met. The orientation guide does not impose any requirements for the purpose of § 8a Para. 5 BSIG.

This document provides answers to the following questions:

- What are the possible approaches for KRITIS operators when fulfilling the obligation to provide verification according to § 8a Para. 3 BSIG? What information should be provided and to whom? (Chapter 2)
- What are the tasks of the auditing bodies? What are appropriate auditing bodies? (Chapter 3)
- What competencies should the audit team have? (Chapter 4)
- How should the audit be performed (audit basis, subject areas, methods, scope, results, comparability)? (Chapter 5)
- How are verification documents submitted and what deadlines must be observed (Chapter 6)?

1.3 Definition of terms[1]

The orientation guide differentiates between the ***audit***, the ***audit report,*** the ***verification - documents*** and the ***verification***.

In this document, the term ***audit*** refers to "security audits, audits or certifications" according to § 8a Para. 3 BSIG. Audits are carried out by an auditing body with the help of an audit team and the results are presented to the KRITIS operator.

The ***audit report*** is the document containing the audit results. The audit report is drawn up by the auditing body and presented to the KRITIS operator. The BSI may request the submission of the documentation on which the review was based (e.g. IT security concepts, process documentation, business continuity management and contingency concepts).

The forms and their appendices that the KRITIS operator submits to the BSI **for each system (or grouped)** are referred to as ***verification documents***. These comprise the following:

- confirmation from the auditing body that the operator complies with the legal requirements of § 8a Para. 1 BSIG and that findings deviating from these are recorded as security deficiencies
- general information on the nature and extent of the audits carried out
- the list of security deficiencies and the implementation plan
- other information required to complete the process

The ***verification*** comprises the complete ***verification documents***.

1.4 Roles and responsibilities in the verification process

The framework conditions and implementation guidelines described within the scope of this orientation guide affect the roles "KRITIS operator", "auditing body", "audit team" and "BSI", which are illustrated in Figure 1.

Auditing bodies may declare their suitability on the basis of appropriate recognition or accreditation or in the form of a self-declaration. The graphic does not illustrate this aspect, since the BSIG does **not** introduce a new approval/accreditation process; it simply refers to existing processes.

[1] Additional definitions of terms can be found in the glossary

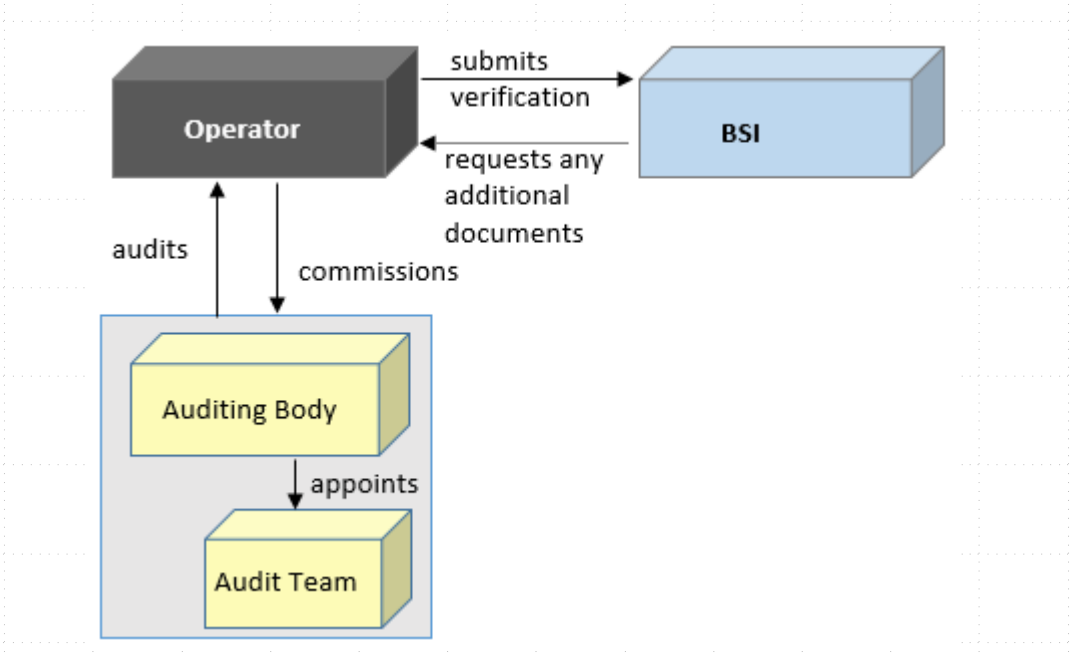

Figure 1: Roles in the verification process, source: BSI

1.4.1 KRITIS operators

Under § 8a Para. 3 BSIG, critical infrastructure operators within the meaning of the BSI Act are required to provide evidence every two years of compliance with the implementation of appropriate organisational and technical precautions (relationship between the effort and the possible consequences of a disruption to the supply service) in accordance with § 8a Para. 1 BSIG. The precautions serve to ensure the functionality of the essential services (kDL) and thus the maintenance of the supply service.

The obligation to take appropriate security precautions in accordance with § 8a Para. 1 BSIG also results in the obligation for the KRITIS operators to commission an auditing body to check the implementation of safeguards in accordance with § 8a Para. 3 BSIG.

1.4.2 Auditing body and audit team

The auditing body puts together a suitable, qualified and independent audit team (see Chapter 4), which prepares and carries out the actual audit and documents it in an audit report. The responsibilities of the auditing body regarding audits and verification are described in detail in Chapter 3.

The auditing body is responsible to the KRITIS operator for the correct execution of the audit (Chapter 6) as well as for the audit report and the corresponding documents.

Due to the shared responsibility of the auditing body towards the KRITIS operator and the KRITIS operator towards the BSI, it is recommended that the obligations between the auditing body and the KRITIS operator are clearly agreed by contract.

1.4.3 BSI

The BSI receives verification from the KRITIS operator, including a list of the security deficiencies with the associated implementation plan for dealing with these deficiencies. The verification shall also include information on the audit carried out, such as a description of the audit object.

The BSI accepts the verification of the KRITIS operator, checks it for completeness and evaluates it initially to see whether its contents are conclusive and informative enough to assess the degree to which requirements have been met. The BSI immediately requests any content and documents that is obviously missing. After submission of the complete documents (i.e. all documents required for the verification review), the KRITIS operator will receive a confirmation of receipt by e-mail stating the new verification period (see also Chapter 6).

In principle, further verification reviews can be carried out up to the submission of the subsequent verification depending on available capacities and at the discretion of the BSI. The BSI does not assess the quality of the content of the verification.

If no further enquiries are necessary for verification or no further cooperation of the KRITIS operator is required for subsequent auditing, the KRITIS operator will not receive any further notification of the procedure after the confirmation of receipt detailed above. The BSI can, however, request further parts or the entire documentation on which the audit is based at any time, or schedule on-site audits, irrespective of the specific reason.

2 The KRITIS operator

The KRITIS operator must guarantee compliance with the requirements according to § 8a Para. 1 BSIG (appropriate provisions in order to avoid errors in compliance with the state of the art) for their systems. To do this, they must first define a suitable scope for the audit object, determine the underlying processes and plan, implement and document appropriate security safeguards.

In order to demonstrate the implementation of safeguards, they must commission an appropriate auditing body, which carries out the audit of one or more systems of the KRITIS operator (audit or certification) and provides the results in writing to the KRITIS operator in an audit report listing the security deficiencies found.

In the next step, the KRITIS operator submits the verification to the BSI at least every two years. Verification must be provided for each system in accordance with the BSI Regulation on the Determination of Critical Infrastructures (BSI KRITIS Regulation). If several systems are comparable and many test steps are carried out together, the information can also be summarised in one form.

The following section includes answers to the following questions:

- What does the scope cover? (Section 2.1)

- What documents should the KRITIS operator provide the auditing body with in order to implement the audit? (Section 2.2)
- Which audit bases can be used? (Section 2.3)

2.1 Description of the audit object

An appropriate audit must include the entire scope[2] of the critical infrastructure as the audit object, i.e. the system according to BSI-KritisV. The scope must therefore be precisely defined and described in preparation for the audit[3]. In addition, essential points of this description can also be listed in form PD of the verification documents.

For the implementation of the audit and the verification, the following should be described:

- the system
- the parts of the essential service provided by the KRITIS operator
- the parts of the essential service provided by external service providers (e.g. outsourcing)
- the interaction with other systems
- the interfaces and dependencies

For the implementation of the audit, all of the following should be listed:

- IT systems
- components
- processes
- roles, persons and organisational units

In particular, the list should include what is necessary for the functioning of the essential service provided or which (may) influence its functioning.

2.2 Standard security documentation

In order for the audit team to be able to properly carry out the audit for the verification according to § 8a Para. 3 BSIG, it requires concrete documents and the option of an on-site inspection involving a visual inspection of the technology and the option of talking to employees of the KRITIS operator (see also Chapter 6).

For checking the official documents, KRITIS operators should provide the auditor, for example, with the following documents[4]:

- Security concept (incl. presentation of implemented and planned safeguards, in particular industry-specific safeguards and KRITIS security objectives derived from the essential services)

2 See “Scope” in the Glossar
3 Additional information can be found in the orientation guide to B3S, Chapter 1: Scope
4 The orientation guide to the B3S includes additional information on the documents required.

- Description of the information security management system (ISMS)
- Contingency concept and description of continuity management
- Asset management documents
- Documentation of the processes for structural and physical security (e.g. site access control or fire protection safeguards)
- Documentation of the personnel and organisational security (e.g. records on employee training measures, awareness-raising campaigns, authorisation management)
- Concepts and documentation for incident identification and processing (e.g. description on incident management, detection of attacks, forensics)
- Concepts and documentation of reviews (e.g. audit reports of the internal audit and of other audits performed, drills, systematic log analyses, etc.)
- Guidelines on external information supply
- Guidelines on dealing with suppliers and service providers (e.g. service level agreements and other security-relevant agreements with service providers)

The auditing body may use additional documents as the basis of the audit.

2.3 Selection of the audit basis

In consultation with the auditing body, the KRITIS operator selects the audit basis. The following cases can be distinguished, among others, which are described in more detail in Section 5.1 on carrying out audits, whereby the cases are not mutually exclusive:

- audit based on a suitable industry-specific security standard (B3S) (Section 5.1.1)
- audit without using any industry-specific security standard (B3S) (Section 5.1.2)
- consideration of existing audits or other audit bases (Section 5.1.3)

3 The auditing body

An auditing body is an appropriate institution commissioned by the KRITIS operator to determine whether the operator has taken appropriate provisions in line with to § 8a Para. 1 BSIG.

In order for an auditing body to be considered appropriate, it should meet the technical and organisational requirements described in this chapter. Specifically, the auditing body appoints the audit team performing the actual audit. The auditing team should have the competencies described in Chapter 4.2.

This section includes answers to the following questions:

- What are the tasks of the auditing body? (Section 3.1)
- When is an auditing body appropriate? (Section 3.2)
- What kinds of auditing bodies are there? (Section 3.3)

3.1 Tasks

The auditing body must perform the following tasks:

- confirm compliance with the processes and methods
- ensure a consistent and equivalent implementation of the audit and audit results
- perform the quality assessment
- define framework conditions for the implementation of the audit (audit processes, etc.)
- assemble the audit team and ensure coverage of all areas of competence
- confirm the suitability of the auditors
- implement the communication with the KRITIS operator on the one hand, and with the audit team on the other

The auditing body assumes the responsibility for the audit results, signs the test documents and sends them to the KRITIS operator.

3.2 Qualification

An auditing body is suitable if the following criteria are met:

- The necessary processes (e.g. information security management system (ISMS), quality assurance procedures, documentation and recording procedures, archiving and backup concept, audit process) must be introduced, implemented and documented in concepts.
- The auditing body must carry out each audit in line with the documented audit process. The uniform understanding of deviations is absolutely essential for assessing the deficiencies. If a security deficiency is assessed as a severe deviation, the reasons must be analysed and documented comprehensibly.
- It must be ensured that each audit is independent and impartial, neutral and free of instructions.
- Compliance with the ethical principles (see appendix) must be ensured.
- The type and extent of the audit actions and results are documented uniformly, objectively and properly.
- Sufficiently competent human resources and suitable infrastructures are made available. An auditing body must meet the following criteria:
  - have at least one manager and one deputy in order to be able to compensate for planned and unplanned management absences
  - carry out the audit procedure within a reasonable period of time
  - be able to demonstrate secure infrastructure, systems, applications and a secure IT network structure
- The auditing body shall have a defined process in place to determine the competence of the audit team and other persons involved in conducting the audits(e.g. technical experts). The following competencies must be available in the audit team for this:
  - reliable knowledge of the field of information security
  - industry expertise and technical know-how in the field of providing the essential services of the audited KRITIS operators
  - reliable knowledge in the field of management systems and particularly information security management systems (ISMS)
  - detailed knowledge of the requirements of audits in line with § 8a Para. 3 BSIG

All auditors must comply with ethical principles such as trustworthiness, objectivity, independence and diligence (see Appendix "Basic ethical principles").

In order to provide for a comparable quality of the audit results, the audits should be performed within the verification framework on the basis of common standards. Compliance with the requirements regarding the auditing body and the implementation of the processes should be checked by an independent authority.

An auditing body may be deemed appropriate if it has demonstrated its neutrality and qualification to this independent authority.

In many cases, the auditing body does not have to prove to the BSI that the aforementioned suitability criteria have been met, as they are already subject to a recognised accreditation regime. A list of suitable auditing bodies is given in the following chapter.

If an auditing body is not included in this list, individual proof of suitability can also be provided by a self-declaration to the BSI in exceptional cases.

3.3 Overview of appropriate auditing bodies

The auditing body may demonstrate its qualification with the following, for example:

- an accreditation with the DAkkS (German National Accreditation Body) for ISO/IEC 27001 certification (accredited certification bodies of the DAkkS) (Section 3.3.1)
- a certification as IT security service provider or an approval as auditing body with the BSI (Section 3.3.2)
- an external quality assessment according to "International Standards for the Professional Practice of Internal Auditing" (IIA)[5] and/or DIIR auditing standard no. 3 "Examination of Internal Auditing Systems (Quality Assessments)" (DIIR)[6] (Section 3.3.3)
- an accreditation as an accounting institution by the IDW (Section 3.3.4)
- an individual verification of suitability by self-declaration to the BSI (Section 3.3.5)

In addition, it should be demonstrated that the members of the audit team as a whole have all the necessary competencies (see Chapter 4).

The qualifications of the auditing body are described in more detail in the sub-sections below.

3.3.1 Accredited certification bodies of the DAkkS

Within the scope of an ISO/IEC 27001 certification process, the DAkkS assumes the function of the "independent authority". A qualified certification body is accredited for the field of ISO/IEC 27001 and must demonstrate the implementation and compliance of the ISO/IEC 17021-1 and ISO/IEC 27006 standards to the DAkkS. These bodies thus fulfil the necessary quality requirements.

An overview of the bodies accredited for ISMS certification in Germany can be found on the website of the German National Accreditation Body (DAkkS).

3.3.2 Certified IT security service providers or approved auditing bodies of the BSI

The BSI offers certification of IT security service providers for various areas of application. Irrespective of the scope, the aim of recognition by the BSI is to ensure the professional competence, quality and comparability of the concepts, procedures and work results of the auditing bodies. A prerequisite for certification as an IT security service provider is meeting

5 http://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2015_Standards_V3.pdf
6 http://www.diir.de/fileadmin/fachwissen/standards/downloads/DIIR_Revisionsstandard_Nr_3.pdf

the requirements of DIN EN ISO/IEC 17025 in the respective valid version. The procedure for certification or recognition of auditing bodies is laid down in a published description of the procedure, which is supplemented by an audit catalogue[7].

These bodies therefore meet appropriate quality requirements. The BSI website contains a list of auditing bodies and IT security service providers that are recognised or certified by the BSI.

3.3.3 Internal audits

Internal audits can demonstrate an appropriate and efficient auditing system and compliance with the International Standards for the Professional Practice of Internal Auditing of the Institute of Internal Auditors (IIA) by means of a quality assessment (QA). In this case, the independent authority is the body performing the QA audits. This procedure is based on DIIR[8] revision standard no. 3 "Audit of Internal Audit Systems (Quality Assessments)" and IIA standards 1300ff[9].

In order to assess the appropriateness and effectiveness when auditing the current state of the art, an internal auditing process must also meet certain quality criteria. Compliance with specific criteria is checked within the scope of a quality assessment. The following six minimum requirements must be met:

- An official written, appropriate regulation regarding the implementation of the audit (rules of procedure, audit guideline or similar).
- Neutrality, independence from other functions and unrestricted information rights are guaranteed.
- The internal auditing department has the appropriate quantitative and qualitative human resources.
- The audit plan for the internal audit is drawn up on the basis of a standardised and risk-oriented planning process.
- The type and extent of the audit actions and results are documented uniformly, objectively and properly.
- The implementation of the safeguards documented in the report is monitored by the internal auditing department using an efficient follow-up process.

By complying with the international standards, the independence of the internal auditing department is guaranteed particularly. Additionally, the code of ethics of the IIA is binding for internal auditors. The requirements regarding integrity, impartiality, confidentiality and professional competence are described here[10].

7 https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Stellen/Stellen_node.html
8 DIIR: German Institute of Internal Auditors
9 http://www.diir.de/zertifizierung/quality-assessment/
10 See http://www.diir.de/fileadmin/fachwissen/standards/downloads/IPPF_2015_Standards_V3.pdf

3.3.4 Accounting institutions

Due to the high level of responsibility that an accounting institution assumes, it fulfils special professional obligations, which are summarised in the Public Accountant Act (WPO)[11]. These include independence, discretion and professional conduct.

3.3.5 Self-declaration to the BSI

If an auditing body is not subject to one of the recognised accreditation schemes described above, it may nevertheless demonstrate its suitability, provided that it fulfils the above suitability criteria as described in Chapter 3.2.

This can be recorded in a self-declaration and presented to the BSI. The auditing body explains in detail in writing how it fulfils the eligibility criteria and how it complies with independence, neutrality, freedom of instruction and other requirements (see Appendix: Basic ethical principles).

The self-declaration is a binding statement of compliance with the criteria and must therefore be in writing and signed by an authorised signatory of the auditing body. It can only be carried out by an auditing body with a commitment to a KRITIS operator and only in connection with a specific request for commissioning by the KRITIS operator (exception: the auditing body is already part of the KRITIS operator as in the case of an internal audit). The self-declaration can be submitted to the BSI prior to the verification process. However, it may also be sent to the BSI together with the other supporting documents.

A general self-declaration by an auditing body is not sufficient. The terms and conditions for each case are individual and require separate consideration.

4 The audit team

The auditing body puts together an audit team that is commissioned with the concrete audit at a KRITIS operator.

The audit team must meet all the requirements necessary to provide the appropriate verification and possess the required competence. In principle, an audit team should consist of at least two qualified employees in order to adhere to the two-person rule. In duly substantiated exceptional cases, for example where an auditor demonstrably possesses all the necessary competencies, an audit team may also consist of a single person.

Depending on the extent of the audit, additional auditors and/or technical experts (e.g. to provide industry-specific or system-specific know-how) may be added to the team. All members of the audit team should comply with the “basic ethical principles” set out in the appendix.

11 See www.wpk.de/pdf/wpo.pdf

4.1 Tasks

An audit team of the auditing body implements the audit according to a specified audit process and draws up an audit report documenting the audit results.

This audit can be performed

- as an individual audit of a suitable (internal or external) auditing body
- as an additional audit, e.g. within the scope of
  - an internal ISMS audit by internal, independent IS auditors (first-party audit)
  - an audit performed by qualified chartered accountants
  - an ISO/IEC 27001 certification, i.e. a certification, monitoring or re-certification audit (native or on the basis of IT-Grundschutz) by auditors (third-party audit)

4.2 Competence and suitability

To enable the auditors commissioned by the KRITIS operator to perform the appropriate audits and thereby provide the appropriate verification to comply with the legal requirements, they must be competent in the following fields:

- Additional audit process competence for § 8a BSIG
- Audit competence
- IT security competence and information security competence, respectively
- Industry competence

An auditor does not have to have all these competences individually; the appropriate composition of an audit team covering all areas of competence is sufficient. If the auditors themselves do not possess the required competence, a technical expert with the appropriate knowledge can also be included in the audit team. Particularly with regard to industry competence, it can be helpful to call in different experts for different areas (e.g. as a member of the audit team or as part of interviews).

Employees of the KRITIS operator or its service provider entrusted with the operation or IT security of the system to be inspected are not eligible as members of the inspection team.

Expert knowledge from this group of people can be collected by the audit team in the course of an interview. However, participation as part of the audit team and thus in the evaluation of

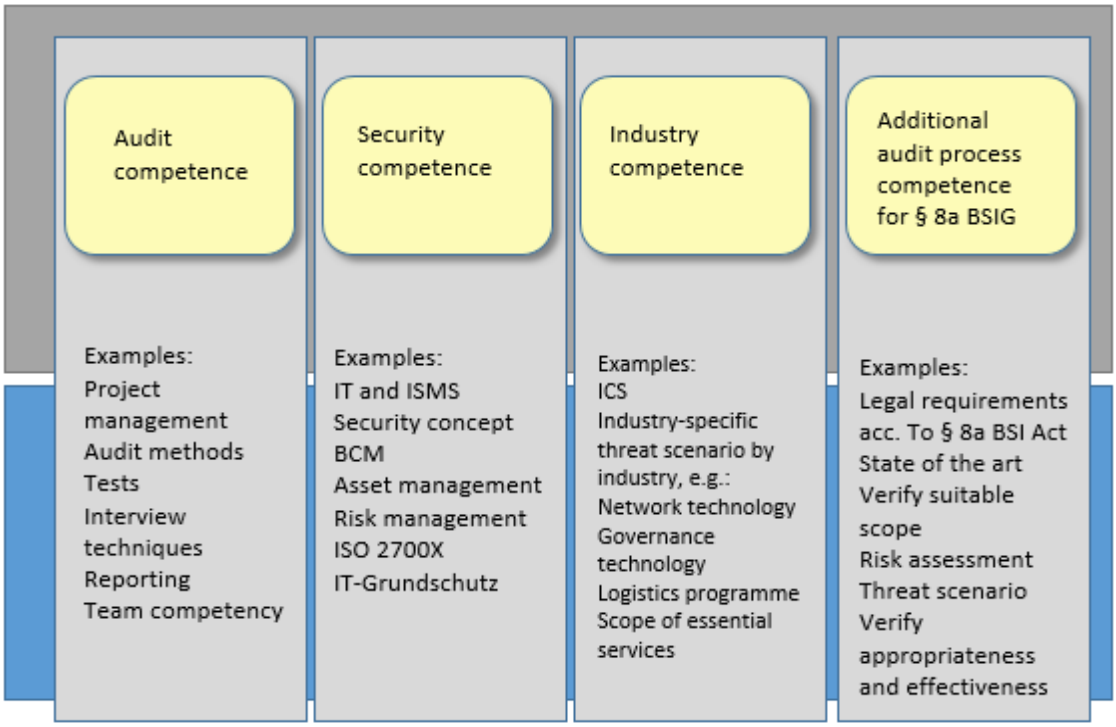

Figure 2: Subject areas of the areas of competence, source: BSI

the facts ascertained within the framework of the audit shall be excluded.

Figure 2 shows the focal subjects that should be present in the individual areas of competence as a minimum requirement.

Note: The overall competence can be shared by several examiners. However, it is important that auditors with a sufficient level of competence are involved in every audit section.

4.3 Acquiring additional audit process competence

By additional audit procedure competence for § 8a BSIG, we mean knowledge of the characteristics of a KRITIS-specific audit within the area of § 8a BSIG. In particular, this concerns the evaluation of the scope, the protection of security of supply, restrictions in risk treatment, the consideration of the "state of the art" and other special aspects that are KRITIS-specific.

This competence can be acquired in a separate training course that deals in deal with the special aspects and requirements of an audit in line with § 8a BSIG. This training is not an accreditation, recognition or certification of an auditor; it is a recommended additional qualification.

5 Performing the audit

The following chapter describes the matters to be taken into account when performing the audit. This includes the KRITIS operator, the auditing body and the audit team. The criteria for an appropriate audit will be listed, with equivalent alternatives possible in particular depending on the technical/professional competence of the auditing body. The following questions will be answered:

- What audit basis has been defined? (Section 5.1)
- Which audit subjects should be audited? (Section 5.2)
- Which auditing methods may be used? (Section 5.3)
- What is the expected time for the audit? (Section 5.4)
- How can the audit schedule and random samples be drawn up? (Section 5.5)
- Which contents should be included in an audit report and the audit documentation, respectively? (Section 5.6)
- Which deficiencies must be documented and which deficiency categories should be used? (Section 5.6)

5.1 Audit basis

As a matter of principle, a plurality of audit bases is possible as long as they are suitable to demonstrate compliance with § 8a Para. 1 BSIG.

5.1.1 Audit when implementing a B3S according to § 8a Para. 2 BSIG

If there is an industry-specific security standard (B3S)[12] with suitability determination from the BSI for the respective scope of application and if it was applied by the KRITIS operator during the implementation of safeguards, it can be used as a reference document for creating the audit plan. A B3S describes both the scope and the minimum requirements of the safeguards to be implemented.

The scope of the audit is determined by the auditor alone or jointly with the KRITIS operator and is based on the individual circumstances of the KRITIS operator on site (at least all systems registered with the BSI must be covered within the scope). The scope of a B3S, however, is typically oriented to the conditions of the entire industry. It is therefore necessary to examine whether the scope of the B3S fully covers that of the audit or if further additional individual safeguards may be necessary. The specifications of the B3S should be mapped to the systems to be audited.

12 See also: https://www.bsi.bund.de/Stand-der-Technik

5.1.2 Audit without implementing a B3S

If there is no B3S or if the audit is to be performed separately from a B3S, it must be ensured that the requirements according to § 8a Para. 1 BSIG are complied with differently. The audit must be suitable to demonstrate the aforementioned. Prior to performing the audit, the auditing body must define a suitable audit process and must comprehensibly document the defined audit process. This audit process will then serve as the audit basis.

Indications for a suitable audit process may include the following:

- the orientation guide to sector-specific security standards (B3S) according to § 8a Para. 2 BSIG
- other B3Ss according to § 8a Para. 2 BSIG whose suitability has been determined (in this regard, the scope of the B3S should be adapted to the scope to be audit, if necessary
- relevant standards (e.g. certification schemes for ISO 27001 (native or on the basis of IT-Grundschutz), ISO/IEC 17021--1, ISO/IEC 27006)

5.1.3 Consideration of existing audits

As a matter of principle, existing audits may be considered when furnishing the verification, i.e. it is possible to cover aspects to be covered for § 8a Para. 3 BSIG within the scope of different audits. In this respect, the audits must be up-to-date, i.e. at the time of filing with the BSI they must have been carried out within one year. Older verifications may be incorporated into the audit in the form of a document analysis (see Section 5.3), but this does not take the place of the current audit (e.g. due to a changed risk situation and efficiency of safeguards). Any outstanding aspects must be incorporated in the proprietary audit plan; in particular, it must be ensured that the scope completely covers the critical infrastructure to be audited and takes additional framework conditions relevant to the critical infrastructure (e.g. dealing with service providers, limitations regarding the risk acceptance) into account. The "Orientation Guide to Industry-Specific Security Standards" provides an indication of such framework conditions.

The responsibility to completely cover the scope rests with the KRITIS operator. The completeness is checked expressly by the auditing body.

5.1.3.1 Use of ISO 27001 certificates for verification

A valid ISO 27001 certificate can be used as part of a verification in line with to § 8a Para. 3 BSIG, as long as some basic conditions are met. This applies both to native ISO 27001 certificates as well as ISO 27001 certificates based on IT-Grundschutz.

An ISO 27001 certification does not automatically cover the entire scope relevant for the verification in line with § 8a BSIG. The scope of the verification must cover the critical infrastructure or the essential service fully (process layer).

In addition, the information security process with regard to the essential service must be viewed through "KRITIS glasses". Avoiding shortage of supplies in essential services is very

important in the context of KRITIS. The essential service must therefore be considered with the focus on avoiding shortage of supplies for the population.

The following section will consider the general framework conditions for the use of ISO 27001 certificates for verification in line with § 8a Para. 3 BSIG:

1. Defining scope
   The scope must include the systems operated according to the BSI KRITIS Regulation. The interfaces should be suitably defined.
2. Extended scope
   The scope must be extended to outsourced areas and a comprehensive security assessment carried out from the KRITIS perspective. This can be based on ISO 27001 or other comparable procedures.
3. Consideration of KRITIS protection objectives
   The BSI Act requires appropriate measures to be taken for the operation-relevant parts of the respective systems in accordance with the protection requirements. Maintaining the security of supply of the population must be the central concern in information security risk management. The requirements placed on the provision of services are also referred to as KRITIS protection objectives. The KRITIS protection objectives of the operation-relevant parts are to be suitably defined. The KRITIS protection objectives (e.g. the availability of the essential service) are to be included in the proprietary risk analysis and additionally considered throughout all processes and safeguard implementations ("KRITIS glasses").
4. KRITIS protection needs
   As part of risk management, therefore, the protection objectives of availability, confidentiality, integrity and authenticity must be assessed in terms of the extent to which the essential service is maintained.
   A purely economic view is not generally sufficient (see "Dealing with risks"). The impact on the functioning of the essential infrastructure and essential service should be considered as an indication of the level of risk to the public. However, it should also be considered that the effort required to implement the safeguards is proportionate to the level of risk for the population.

   Note: § 8a Para. 1 BSIG requires “[...] Precautions to avoid disruption to availability, integrity, authenticity and confidentiality [...]”. Risk management based on the evaluation of confidentiality, integrity and availability, as is usual in ISO 27001 or IT-Grundschutz of the BSI, is possible as long as it is ensured that authenticity is considered in the risk assessment and selection of safeguards.

5. Dealing with risks
   A purely economic consideration of the risks and the protection needs is not generally sufficient. In particular, the level of risk to the public, i.e. the impact on the functioning of the essential infrastructure and essential service, must be taken into account. In selecting safeguards, care must be taken to ensure appropriateness, i.e. the possible consequences of a failure or impairment of public services must be considered in relation to the cost of security precautions.

   - Risk acceptance
     According to § 8a Para. 1 BSIG, risks in scope may not be accepted if state-of-the-art security precautions are possible and appropriate. Risk acceptance is only possible for the remaining residual risk then.
   - Insurability of risks
     A transfer of the risks, e.g. by insurance, is not a substitute for the security precautions according to § 8a Para. 1 BSIG. In the case of insurance or other risk transfer, appropriate security precautions must also be taken in accordance with the state of the art. However, the KRITIS operator is free to take out additional insurance.

6. Implementation of safeguards
   In principle, all safeguards necessary for the maintenance of the essential service must be implemented. All safeguards that are only planned, for example in the continuous improvement process (CIP), in the implementation plan or in the risk treatment plan, must be included in the list of security deficiencies according to § 8a Para. 3 BSIG. In order to assess these deficiencies, explanatory documents such as the deficiency assessment, CIP documentation and implementation plan should also be submitted.

5.1.3.2 Use of an existing C5 attestation

The Cloud Computing Compliance Controls Catalogue (C5) is a minimum standard for IT security for Cloud Service Providers (CSPs). CSPs are classified as essential infrastructures within the “data storage and processing” essential service if the corresponding threshold of the BSI KRITIS Regulation is exceeded. A passed C5 attestation can be used as part of a proof according to § 8a Para. 3 BSIG, as long as some basic conditions (see FAQ to C5[13]) are met during the testing.

5.2 Audit topics and auditing of the scope

Generally, the audit topics are described in detail in the B3S; in particular industry-specific requirements and/or safeguards may be listed there, the implementation of which must be ensured.

13 see https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_8aBSIG_C5/faq_bsi_8a_C5_node.html

If there is no B3S or if no B3S is used for auditing, the audit topics can be derived from the orientation guide for drawing up a B3S. Chapter 5.3 of this orientation guide includes audit topics that must be taken into account.

In particular, verifying that the scope has been chosen correctly is very important for the suitability of the evidence. The auditor must question whether the choice of scope is correct and fully includes the information technology systems, components and processes belonging to the critical infrastructure, as well as those influencing the critical infrastructure.

In this respect, the scope must be evaluated and checked under the audit aspects

- functionality of the essential service
- suitability and necessity and
- completeness

The auditing body shall examine the suitability of the scope within the meaning of § 8a Para. 3 BSIG and present the result in the audit report.

Note: As a matter of principle, it makes sense that the auditing body, together with the KRITIS operator to be audited, clarifies the scope of the audit prior to being engaged, and that the auditing body creates the cost assessment and the offer for the audit on this basis.

5.3 Possible audit methods

The term “audit methods” refers to all methods used to examine a situation. For example, the following different audit methods may be used during an audit:

- personal questioning (interview)
- (visual) inspection of systems, sites, premises and objects
- document analysis (this also includes electronic data)
- technical on-site audit and/or targeted observation (e.g. the functionality of alarm systems, site access controls, having applications demonstrated)
- penetration tests
- data analysis (e.g. log files, firewall configuration, analysis of databases, etc.)
- written questioning (e.g. questionnaire)
- incorporation of existing verification (e.g. reviewing the audit report of an audit performed in a different context, see also Section 5.1.3)

The use of the different audit methods depends on the specific case and must be defined by the audit team.

5.4 Audit effort

The determination of the audit effort for first-time audits includes, for example:

- the size of the scope to be audited, as measured by the number of employees of the organisation
- the criticality and the degree of supply, respectively, according to BSI-KritisV
- the complexity of the scope to be audited
- the IT dependence and the IT penetration, respectively, of the essential service
- the question of whether detailed investigations based on expert/technical tests or analyses should be carried out within the scope of the audit – this will normally be the case if the KRITIS operator does not carry out such tests regularly

In order to estimate the complexity, the following questions may be used:

- How complex is the IT system environment (number of systems and heterogeneity of the systems used)?
- How many sites does the object of examination encompass (scope)?
- How many network transitions are there?
- Which and how many IT applications are being used in the organisation? Do they support critical business processes?
- Are superordinate methods being used that have an influence on areas outside of the organisation?
- How long has the topic of information security been established in the organisation and what is the organisation's level of experience in this respect? Have (partial) systems already been certified, if applicable?

The actual time required for the audit is difficult to estimate, since the systems of KRITIS operators of critical infrastructures can vary greatly.

Each audit should cover the six audit steps listed below. In general, these are to be adapted to the specific system and the sector-specific characteristics.

Audit steps	Activity
Step 1	Preparation of the audit as well as examination of the suitability of the scope
Step 2	Creation of the audit plan
Step 3	Checking of official documents
Step 4	On-site audit
Step 5	Follow-up of the on-site audit
Step 6	Drawing up of the audit report

Table 1: Basic guide to the relative time required to carry out an audit as verification of the implementation of the requirements § 8a Para. 3 BSIG, source: BSI

5.5 Audit plan and possible selection of random samples

Every audit must be based on a documented audit plan. This defines the audit team, the audit objects, the audit goals, as well as the intended audit method prior to the actual audit. Likewise, the roles within the audit team and the necessary contact persons on part of the KRITIS operator as well as the schedule should be defined.

A complete audit of the entire scope at reasonable cost is normally not possible. That is why the auditor must define an appropriate selection of random samples within the audit plan. This selection must at least include all critical processes. The selection of the random samples must be risk-oriented (consideration of likelihood and effects on the provision of the essential service; however, it must be ensured that comprehensive random samples provide good coverage of the system or systems of the critical infrastructure as well as coverage of the network topology. Areas with higher risks should be treated more seriously. The risk assessment should include in particular the impact on the supply of the population with the essential service according to the size of the KRITIS operator (How many people would be affected by a failure? How serious would a failure or malfunction be?) The selection of the random sample must be justified.

Establishing a multi-year auditing concept is recommended so that each IT system, each IT component and each IT process is audited at least once in the foreseeable future. The random sample must be selected by the auditor or the auditing body, respectively. It is not appropriate to use the same random sample for several audits. The audit plan should take into account previous audits in order to achieve a complete coverage of all components/processes in the long run. In particular, the list of deficiencies from the last audit result (audit reports) must be taken into account in the audit plan when selecting the random samples.

Note: The standards ISO 19011, ISO/IEC 27007 and ISO/IEC 27008 may include information for planning and implementing an audit.

5.6 Documentation of the audit result in the audit report

The audit report as part of the verification according to § 8a Para. 3 BSIG on the implementation of the requirements according to § 8a Para. 1 BSIG should meet the following criteria:

- be a separate document
- be drawn up in German[14]
  all contents must be comprehensible
- have an unambiguous denomination and version control
- include all meta information relevant to the evaluation (e.g. scope of the examination, audit goal, time, place and duration of the audit, auditing body and audit team, audit results, etc.)
- document all audit steps on a comprehensible and repeatable basis and set out the audit decisions on a substantiated basis

In particular, security deficiencies and recommendations must be documented in the audit report. The BSI provides a description of the minimum requirements and a model of a list of deficiencies on its websites.

5.7 Security deficiencies, implementation plan and list of deficiencies

5.7.1 Security deficiency

For each tested security precaution in accordance with § 8a Para. 1 BSIG, the established facts shall be included in the list of deficiencies in the audit report and evaluated with regard to the implementation status. If a deviation from the requirements according to § 8a Para. 1 BSIG is found, it is a security deficiency which has to be documented in the list of deficiencies and evaluated with regard to the provision of the essential service. As a matter of principle, all determinations representing a risk or requiring corrective action that cannot be implemented without the use of time or resources must be included in the audit report.

5.7.2 Deficiency categories

To classify security deficiencies, deficiency categories shall be defined and used uniformly throughout the audit report. In this respect, each auditing body may select an evaluation scheme that is standard for its audits. However, uniform deficiency assessments must be made in the list of deficiencies of the verification document sent to the BSI. If the auditor's deficiency categories deviate from the deficiency categories of this orientation guide, the auditor must map their categories to the categories defined in table 2.

14 The audit reports may also be drawn up in English. However, the verification documents must be filed with the BSI in German.

Category	Definition	Audit report / list of deficiencies
Severe or significant deviation/security deficiency	A “severe deviation” is a **serious** threat or a serious risk. A “significant deviation” is a huge threat or a high risk. There is urgent need for action. The deviation must be **eliminated** immediately or promptly, since the confidentiality, integrity, the authenticity or availability of the essential service is severely threatened and significant damage is to be expected.	Incorporation into the audit report and into the verification
Minor deviation/security deficiency	A “minor deviation” is a threat and a risk, respectively. There is no urgent need for action. The underlying deviation must be eliminated in the medium term. The confidentiality, integrity, authenticity or availability of the essential service might be impaired.	Incorporation into the audit report and into the verification
Recommendation	A “recommendation” is a suggestion for improvement. By implementing the recommendation, the security can be increased.[15] Examples of recommendations: - improvement suggestions for the implementation of safeguards - additional safeguards that have been successful in practice - comments regarding the appropriateness and effectiveness of safeguards	Incorporating this into the audit report is recommended No incorporation into the verification required
No deviation	There is no security deficiency if the requirements are complied with in their entirety and if all safeguards have been	No incorporation into the verification required

15 A partially or not implemented measure or requirement, may only be classified as a security recommendation if the audit team have reason to believe that, in the medium term, no impairment of the confidentiality, integrity or availability of the essential service data is expected.

Category	Definition	Audit report / list of deficiencies
	implemented completely, efficiently and appropriately. There is no supplementary information.	

Table 2: Deficiency categories

For the later traceability of the security deficiencies and their classification by the responsible regulatory authorities, it is absolutely necessary that there is a uniform understanding of individual deviations for assessing the deficiencies.

If a security deficiency is assessed as a severe deviation, the reasons must be analysed and documented comprehensibly.

5.7.3 Risk assessment and implementation plan

The security deficiencies must be subject to a risk assessment. The concrete safeguards to be implemented, the persons responsible for them, the planned dates for rectifying the deficiencies, and their implementation status must be specified in an implementation plan.

5.7.4 List of deficiencies

Finally, the list of deficiencies summarises the security deficiencies and their classification, the risk assessment and the implementation plan in a clear manner and also shows the status of implementation. The BSI provides a template for such a list of deficiencies[16] in the download area on its KRITIS web pages. An extract from this template is shown in Table 3.

The list of deficiencies is part of the verification documents according to § 8a Para. 3 BSIG and must be sent by the KRITIS operator to the KRITIS office of the BSI as an attachment to the verification forms.

The KRITIS operator must provide the BSI with sufficient information to assess the respective security deficiencies.

- The security deficiency must be described in a comprehensible manner. It must be clear to the BSI why the circumstance described represents a security deficiency.
- The BSI must be able to understand the (potential) impact of the security deficiency on the availability, integrity, authenticity or confidentiality of the information technology systems, components or processes necessary for the functioning of the critical infrastructure.

16 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/IT_SiG/Maengelliste_PEA_Final.html

- The BSI must be able to trace whether a (serious) security deficiency is properly addressed by the KRITIS operator on the basis of the implementation plan.

The list of deficiencies in the implementation plan may also be extended by the operator by a Comments column for the operator to detail any possible divergences.

Example: No automatic screen locks are activated for medical devices in the operating area of a hospital. The auditor has classified this as a minor deviation. However, the operator can then comment that this is a particularly access-protected area, where an automatic screen lock can even be counterproductive.

					Implementation plan[17]			
ID[18]	**Deficiency description**[19]	**Classification of the deficiency**[20]	**KRITIS reference**[21]	**KRITIS risk**[22]	**Safeguards**	**Persons responsible**	**Time period**	**Status**
1	The corporate policy on password complexity is not applied to ERP systems. Users, especially administrators, are obliged to use complex passwords for organisational reasons. However, this is not technically enforced.	Minor deviation	ERP system for treatment/ordering/distribution/circulation	Taking over a privileged account can have a significant impact on the availability of the essential service, but administrative access is only possible from an isolated and secured administration network. Non-privileged accounts have limited rights and can only cause minor disruption. Anomalies would be detected and promptly controlled by a SIEM.	The adoption of the password guidelines is commissioned as a change by the ERP manufacturer	IT security officers (IT-SiBe), ERP manufacturers, ERP administration	Q3 2018	50%
...	...	...	...	...	...	...	...	...

Table 3: Extract from list of deficiencies template with implementation plan

17 Implementation plan: action plan and timetable for remedial action; with responsibility if required
18 A unique reference or identifier to facilitate communication of deficiencies
19 Deficiency description: A comprehensible description of the security deficiency with a summary heading
20 Classification of the deficiency: the deficiency category (according to the BSI's Orientation Guide to Verification) to assess the risk to the availability, integrity, authenticity or confidentiality of the information technology systems, components or processes necessary for the critical infrastructure to function
21 KRITIS reference: Reference to the part of KRITIS, including a specific reference to the audited system on which the security deficiency has or could have a concrete effect. Limited to the most important subsystems or an overview-like description if there are far-reaching effects
22 KRITIS risk: An assessment of the security deficiency, described in words or as a classification, for the provision of the essential service

6 The verification process in line with § 8a Para. 3 BSIG

Under § 8a Para. 3 BSIG, operators of critical infrastructures shall demonstrate compliance with the requirements of § 8a Para. 1 BSIG in an appropriate manner at least every two years.

6.1 Calculating the verification periods

The BSI Act stipulates that operators of critical infrastructures must take precautions and safeguards to implement § 8a Para. 1 BSIG at the latest two years after the entry into force of the BSI-KritisV and that corresponding verification must be provided in accordance with § 8a Para. 3 BSIG at least every two years.

6.1.1 First evidence after exceeding the thresholds

Operators of critical infrastructures that fall under the regulations of the BSIG for the first time must provide the verification according to § 8a Para. 3 BSIG within two years. The obligation to implement the security safeguards, on the other hand, exists immediately.

6.1.2 Subsequent verification and implementation deadlines

Operators of critical infrastructures that are already covered by the BSIG and have provided verification for the first time in accordance with § 8a BSIG must continue to provide subsequent verification every two years. In principle, the verification process is ongoing, i.e. the submission of verification immediately leads to the obligation to provide subsequent verification. When calculating the time periods, the date of the first submission is definitive.

If a verification proves to be unsuitable or incomplete in the course of the BSI review and additional submissions are required, this does not affect the period calculated initially for the subsequent verification.

Submission of subsequent verification:

When a verification is submitted, a calculation is always made based on the exact date of the submission, which is communicated to the operator in the confirmation of receipt. The date for submission of subsequent verification is calculated from the original submission date, plus two years. Whether all necessary verification documents were actually submitted at the time of submission (see Chapter 6.2.2 "Which supporting documents are to be submitted?") or whether documents are submitted subsequently does not affect the calculation of the time period.

Example:

- Expiry of the period for providing the first verification according to § 8a Para. 3 BSIG ("first basket"): 03/05/2018
- Submission of the verification documents: 15/04/2018
- Expiry of the period for providing the subsequent verification according to § 8a Para. 3 BSIG: 15/04/2020

A KRITIS operator can submit the verification documents at any time before the end of the verification period. If, for example, a KRITIS operator wishes to adapt its obligation to provide evidence in accordance with § 8a Para. 3 BSIG to its annual ISO 27001 audit cycle and carry out the audits jointly, it may also submit its evidence annually. The statutory two-year regulation is a minimum requirement.

6.2 Submission of the verification documents

KRITIS operators must confirm to the BSI that the requirements of § 8a Para. 1 BSIG have been met by submitting the corresponding verification. In order to assess the appropriateness of the audit, the suitability of the provisions for the prevention of errors and the severity of the security deficiencies identified, the verification documents must contain all the required information.

6.2.1 Who submits verification documents?

The KRITIS operators provide the BSI with information on the type and scope of the audit carried out for each system and a list of the security deficiencies discovered during the audit. These verification documents must be submitted to the BSI in writing.

6.2.2 Which supporting documents are to be submitted?

In order to clearly present all necessary information on the type and scope of the audit carried out and to simplify the process of recording, the BSI provides special verification forms and recommends their use when submitting verification documents. The forms, including the necessary attachments, form the cornerstone of the verification sent by the KRITIS operators to the KRITIS office of the BSI. They include the following four forms:

- KI form: information on the audited critical infrastructure and the contact person
- PS form: information on the auditing body and the audit team
- PD form: information on the implementation of the audit
- PE form: information on the audit result and the security deficiencies identified

The KI form must be completed and signed by the KRITIS operator. The PS, PD and PE forms must be completed and signed by the auditing body. The forms are published on the BSI websites at https://www.bsi.bund.de/Nachweise.

KRITIS operators with several systems can submit verification documents to the BSI grouped together for all systems. However, the supporting documents for individual systems can also be submitted separately. It is important, however, that a KRITIS operator always provides and submits the verification documents for all its systems that are currently in the verification process.

The submission of the audit report is not a mandatory requirement when submitting the verification documents initially. A KRITIS operator is only required to submit the detailed audit report to the BSI as an additional submission when this is requested by the BSI.

6.2.3 How can verification documents be submitted?

Verification documents must be submitted to the BSI KRITIS office as the central point of contact. In principle, verification can be sent by post or e-mail to the KRITIS office (kritis-buero@bsi.bund.de). The BSI recommends encrypting the verification documents for confidential transmission by e-mail. The required public S/MIME certificate or the PGP key of the KRITIS office are provided in the download area on the BSI website[23].

6.2.4 Response and confirmation of receipt from the BSI

KRITIS operators will receive a confirmation of receipt from the BSI for submitted verification documents as soon as these have been successfully checked for completeness. The confirmation of receipt shall state the date and the systems for which verification documents were submitted and shall be deemed formal proof that the KRITIS operator has complied with its legal obligation to submit the verification documents pursuant to § 8a Para. 3 BSIG. It also contains the date on which the KRITIS operator must provide subsequent verification (for the calculation of this date, see Chapter 6.1).

The KRITIS operator does not receive any further notification of the procedure from the BSI.

If no further enquiries are necessary for verification or no further cooperation of the KRITIS operator is required for subsequent auditing, the KRITIS operator will not receive any further notification of the procedure after the confirmation of receipt detailed above. The BSI can, however, request further parts or the entire documentation on which the audit is based at any time, or schedule on-site audits, irrespective of the specific reason.

In principle, further verification reviews can be carried out up to the submission of the subsequent verification depending on available capacities and at the discretion of the BSI. As this procedure does not provide for the completion of the verification review, the BSI does not issue any confirmation of the completion of the verification review.

23 https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Downloads/it-sig_downloads_node.html

6.2.5 Additional submissions

In the course of verification reviews, the BSI may request certain documents. The BSI reserves the right to request additional documents at any time even after the confirmation of receipt has been sent. Subsequent requests are generally given with a submission deadline that depends on the type and scope of the additional submission.

Additional submissions do not affect the period calculated for the subsequent verification.

6.2.6 Audits by the BSI

In accordance with § 8a Para. 4 BSIG, the BSI can check if the critical infrastructure operator meets the requirements of § 8a Para. 1 BSIG. BSI audits can be routine or triggered by specific reasons. They may be caused, for example, by random samples or discrepancies in the documents submitted in accordance with § 8a Para. 3 BSIG, which the BSI would like to clarify with the operator. An on-site audit at the operator's premises is an essential part of these reviews.

Appendix

Basic ethical principles

In order to create confidence in an objective audit, compliance with the “basic ethical principles” is necessary. Both the individual auditors and the auditing body must comply with the “basic ethical principles”. They include the following principles:

- **Integrity and confidentiality**
  Integrity establishes trust and thereby creates the basis for the reliability of a decision. Since sensitive business processes and information can often be found in the environment of information security, the confidentiality of the information obtained within the scope of an audit and the discrete handling of the information and results of the audit are essential. Auditors appreciate the value and the ownership of the information obtained and do not disclose this information without the corresponding authorisation, unless there are legal or professional obligations to do so.
- **Technical competence**

  Auditors only assume those tasks they have the necessary knowledge, skills and the corresponding experience for and use the aforementioned when doing their work. They continuously improve their know-how and the efficiency and quality of their work.
- **Impartiality and diligence**
  An auditor must demonstrate the utmost expert impartiality and diligence when merging, evaluating and forwarding information about audited activities or business processes. All relevant circumstances have to be assessed on a balanced basis and may not be influenced by the auditor’s own interests or by third parties.
- **Objective reporting**
  An auditor is obliged to provide the customer with true and accurate reports of the examination results. This includes objective and comprehensive reporting of the circumstances in the audit reports, constructive evaluation of the circumstances reported and specific recommendations for improvement of the safeguards and processes.
- **Verification and comprehensibility**
  The rational basis necessary in order to arrive at reliable and comprehensible conclusions and results is the unambiguous and logical documentation of the circumstances. This also includes a documented and comprehensible methodology (audit plan, report) used by the audit team in order to arrive at their conclusions.
- **Independence and neutrality**
  An auditor must carry out the audit impartially and free of instruction. The audit results must be documented comprehensibly. Each audit team should consist of at least two auditors in order to guarantee independence and impartiality (“two-person rule”). For reasons of independence and neutrality, the members of the team must not have previously

been directly involved in an advisory or executive capacity in the audited area, e.g. in the creation of concepts or the configuration of IT systems.

Glossary

Term	Definition
Appropriate	Organisational and technical provisions shall be appropriate if the time and expense required are not disproportionate regarding the consequences of failure or an impairment of the critical infrastructure concerned.
Audit object/scope	The audit object/scope comprises the IT systems, components and processes, roles and persons, respectively, that are key for the functionality of the critical infrastructures operated and which influence these (see also “Scope”).
Audit plan	The document where the auditor defines the framework conditions for the audit before starting the audit. The contents include the audit process and the audit methods, respectively, and defined random sampling.
Audit processes	The method according to which the auditing body provides the verification.
Audit report	Document of the auditing body containing the entire audit or certification results.
Auditing	The appropriate verification that the safeguards have been implemented by the KRITIS operator. It is performed by independent and qualified auditors of an auditing body. The term “audits” includes audits and certifications according to § 8a Para. 3 BSIG.
Auditing body	An organisation that provides verification that the KRITIS operator has implemented the safeguards according to § 8a Para. 1 BSIG.
Competence	A trained skill allowing a person to perform certain work.
Critical infrastructure	See definition in BSI Act or specification in the BSI KRITIS Regulation
Deviation	Non-conformity Indicated security deficiencies are considered deviations.
First-party audit	Sometimes also referred to as internal audits. These are performed by the organisation itself or on behalf of the organisation for internal purposes and may form the basis for the proprietary declaration of conformity of the organisation.
Industry-specific security standard (B3S)	A security standard the suitability of which was determined according to § 8a Para. 2 BSIG (see approval process).
KRITIS operators	A company operating a critical infrastructure according to the ordinance Regulation to § 10 Para. 1 BSIG (BSI-KritisV).

Term	Definition
Monitoring body	Organisation that assumes the supervisory function for an auditing body.
Safeguards	The appropriate organisational and technical provisions which must be implemented as a legal requirement designed to avoid disturbances to the availability, integrity, authenticity and confidentiality of IT systems, components or processes according to § 8a Para. 1 BSIG. These provisions also include infrastructural and personnel safeguards. Particularly critical processes require specialist security safeguards.
Scope	Area covered by an industry-specific security standard (see also "Audit object/scope").
Security deficiencies identified	Necessary safeguards identified within the scope of the audit that have been only partially implemented or not implemented at all. Security deficiencies identified must be assigned “degrees of severity” accordingly (see deficiency categories).
System	Critical infrastructure as defined in the BSI KRITIS Regulation
Third-party audits	Audits that are performed by external independent organisations. Such organisations offer certification or review of the conformity with the requirements.
Verification	The certificate issued by an independent third party regarding the
Verification document	The forms and their appendices, including the results of the audits or certifications carried out, including the security deficiencies